WHAT IS CLAIMED IS:

1. An intrusion preventing system which prevents an intrusion to regular data storage means connected to a network, comprising:

decoy data storage means which is provided separately from the regular data storage means; and

guiding means which guides an illegal access to the regular data storage means into the decoy data storage means.

2. An intrusion preventing system according to claim 1, wherein the regular data storage means and the decoy data storage means are respectively a regular region and a decoy region secured in different regions on the same server.

3. An intrusion preventing system according to claim 2, further comprising destination rewriting means which rewrites a destination of an access which is the server to the decoy region.

4. An intrusion preventing system according to claim 2, further comprising response rewriting means which rewrites the content of a response command returned in response to an access to the decoy region to the content

of a response command which is to be returned in response to an access to the regular region.

5. An intrusion preventing system according to claim 3, further comprising illegal access monitoring means which monitors whether or not an access whose destination is the regular region is an illegal access, wherein

the destination rewriting means rewrites the destination of an illegal access to the decoy region.

6. An intrusion preventing system according to claim 3, further comprising access target monitoring means which monitors whether or not the destination of an access command is the regular region, wherein

the destination rewriting means rewrites the destination of an access command which is the regular region to the decoy region.

7. An intrusion preventing system according to claim 3, further comprising command monitoring means which monitors whether or not an access command includes a mala fide program which performs alteration or erasure of the content of the regular region, substitution of the content

to other data, or the like, wherein

the destination rewriting means rewrites the destination of the access command including the mala fide program to the decoy region.

8. An intrusion preventing system according to claim 2, wherein the regular region and the decoy region are allocated with a common IP address.

9. An intrusion preventing system according to claim 2, further comprising means which collects action logs or trace data of a session guided to the decoy region.

10. An intrusion preventing system according to claim 1, wherein the regular data storage means is a regular server, and the decoy data storage means is a decoy server provided together with the regular server.

11. An intrusion preventing system according to claim 10, further comprising

intrusion judging means which judges whether or not a communication session established between the regular

server and an external terminal is due to intrusion;

communication session relaying means which relays a communication session which has been judged as an intrusion from the regular server to the decoy server; and

path switching means which transfers a packet whose destination is the regular sever to the decoy server in a communication session which has been judged as the intrusion.

12. An intrusion preventing system according to claim 10, further comprising means which rewrites a response command returned from the decoy server into the content of a response command which is to be returned in response to an access to the regular server.

13. An intrusion preventing system according to claim 10, wherein the decoy server is a mirror server of the regular server.

14. An intrusion preventing system according to claim 11, wherein the communication session relaying means comprises

a buffer for transfer which sequentially transfers the same packets as packets whose destinations are the regular

server to the decoy server; and

a buffer for return which sequentially stores responses returned from the decoy server in response to the transferred packets, wherein,

when the communication session which has been judged as the intrusion is relayed to the decoy server, the buffer for return sequentially outputs the responses from the first packet which has been returned in response to the first packet transferred after relayed.

15. An intrusion preventing system according to claim 11, wherein the communication session relaying means comprises

a buffer for transfer which sequentially stores the same packets as packets whose destinations are the regular server; and

a buffer for return which sequentially returns responses returned from the decoy server, wherein,

when the communication session which has been judged as the intrusion is relayed to the decoy server, the buffer for transfer sequentially outputs the responses from the first packet which has been returned in response to the first packet transferred after relayed.

16. An intrusion preventing system according to claim 11, further comprising pseudo response means which, without transferring a packet whose destination has been converted from the regular server to the decoy server, creates a response command to the packet in a pseudo manner to return the same.

17. An intrusion preventing system according to claim 11, wherein, when a source address of a communication session which has been judged as intrusion is stored and a packet containing the source address is then input, a communication session is established between the decoy server and the user.

18. An intrusion preventing system according to claim 11, wherein in the communication session established between the decoy server and the user, action logs and trace data of the user are collected.

19. An intrusion preventing system according to claim 11, wherein the path switching means includes means which converts the content of the response command returned from the decoy server to the content of a response command which will be output when the regular server receives a packet.

20. An intrusion preventing system which prevents an intrusion to a regular region of a server connected to a network, wherein

without allowing access to the regular region for an access command whose destination is the regular region, a pseudo response command expressing a message where the access to the regular region has been succeeded is returned response to the access to the regular region.